We claim:

1. A communication system comprising:

a plurality of multicast devices forming a shared multicast distribution tree;

a host device; and

a designated device through which the host device accesses the shared tree, wherein:

the host device obtains access information for the host device to access the shared tree;

the designated device obtains the access information for the host device to access the shared tree;

the host device sends an access control message to the designated device to join the shared tree; and

the designated device uses the access information to authenticate the host device before adding the host device to the shared tree.

2. The communication system of claim 1, further comprising a key server for authenticating the host device and generating the access information for the host device to access the shared tree.

3. The communication system of claim 2, wherein the key server provides the access information to the host device over a secure communication channel.

4. The communication system of claim 2, wherein the key server provides the access information to the designated device using a unicast distribution mechanism.

5. The communication system of claim 2, wherein the key server provides the access information to the designated device using a multicast distribution mechanism.

6. The communication system of claim 2, wherein the key server provides the access information to the designated device using a broadcast distribution mechanism.

7. The communication system of claim 2, wherein the designated device requests the access information from the key server upon receiving the access control message.

8. The communication system of claim 2, wherein the key server provides the access information to the plurality of multicast devices forming the shared tree.

9. The communication system of claim 1, wherein the access information comprises:
a token identifier; and
an authentication key.

10. The communication system of claim 9, wherein the access control message comprises the token identifier.

11. The communication system of claim 10, wherein the access control message is an Internet Group Management Protocol (IGMP) join request including the token identifier.

12. The communication system of claim 1, wherein the designated device joins the shared tree on behalf of the host device upon authenticating the host device.

13. The communication system of claim 12, wherein the shared tree is a Protocol Independent Multicast (PIM) shared tree, and wherein the designated device sends a PIM join request upstream toward a rendezvous point device in order to join the shared tree on behalf of the host device upon authenticating the host device.

14. The communication system of claim 1, wherein the designated device forwards the access control message to a neighboring device upon failing to authenticate the host device using the access information.

15. The communication system of claim 14, wherein the neighboring device obtains the access information and authenticates the host device using the access information.

16. A method comprising:

authenticating a host device;

generating access information for the host device to join a multicast group;

sending the access information to the host device; and

sending the access information to a designated device for the host device.

17. The method of claim 16, wherein the access information comprises:

a token identifier; and

an authentication key.

18. The method of claim 17, wherein the access information further comprises an expiration date for the authentication key.

19. The method of claim 17, wherein the access information further comprises a public key.

20. The method of claim 16, wherein sending the access information to the host device comprises:

sending a communication message including the access information to the host device over a secure communication channel.

21. The method of claim 20, wherein the communication message is a group key management communication message.

22. The method of claim 16, wherein sending the access information to the designated device for the host device comprises:

sending a communication message including the access information to the designated device over a secure communication channel.

23. The method of claim 22, wherein the communication message is a unicast communication message addressed to the designated device.

24. The method of claim 22, wherein the communication message is a multicast communication message addressed to a multicast group of which the designated device is a member.

25. The method of claim 22, wherein the communication message is a broadcast communication message.

26. The method of claim 16, wherein generating the access information comprises:
generating an access token including the access information.

27. The method of claim 26, wherein the access token comprises:
a group identifier for identifying a multicast group;
a host identifier for identifying the host device;
a token identifier for identifying the access token;
an authentication key for the host device;
an expiration date for the authentication key;
a server identifier for identifying a key server; and
a public key for the key server.

28. A method comprising:

obtaining access information for joining a multicast group from an access information server;

generating an access control message for joining the multicast group using the access information; and

sending the access control message to a designated device for joining the multicast group.

29. The method of claim 28, wherein the access information comprises:

a token identifier; and

an authentication key.

30. The method of claim 29, wherein generating the access control message using the access information comprises:

including the token identifier in the access control message.

31. The method of claim 28, further comprising:

generating authentication information using the access information; and

sending the authentication information to the designated device.

32. The method of claim 31, wherein generating the authentication information using the access information comprises generating a digital signature using the access information and a predetermined digital signature scheme.

33. The method of claim32, wherein the predetermined digital signature scheme comprises a keyed hash function.

34. The method of claim 33, wherein the keyed hash function comprises IPsec AH with HMAC-MD5.

35. The method of claim 33, wherein the keyed hash function comprises IPsec AH with HMAC-SHA1.

36. The method of claim 29, wherein the access information further comprises a token identifier.

37. The method of claim 36, wherein generating the access control message using the access information comprises:

including the token identifier in the access control message.

38. The method of claim 37, wherein the access control message is an Internet Group Management Protocol (IGMP) join request message including the token identifier.

39. The method of claim 28, further comprising:

establishing a security agreement with the designated device using the access information.

40. A method comprising:

receiving an access control message from a host device;

determining whether the host device is authorized to access a shared multicast distribution tree based upon access information for the host device; and

joining the shared tree on behalf of the host device if the host device is determined to be authorized to access the shared tree.

41. The method of claim 40, further comprising:

obtaining the access information for the host device.

42. The method of claim 41, wherein obtaining the access information for the host device comprises:

receiving the access information from an access information server prior to receiving the access control message from the host device.

43. The method of claim 41, wherein obtaining the access information for the host device comprises:

requesting the access information from an access information server after receiving the access control message from the host device.

44. The method of claim 40, wherein determining whether the host device is authorized to access the shared tree comprises:

maintaining an access information database;

searching the access information database for the access information for the host device;

failing to find the access information for the host device in the access information database; and

determining that the host device is not authorized to access the shared tree.

45. The method of claim 40, wherein determining whether the host device is authorized to access the shared tree comprises:

maintaining an access information database;

searching the access information database for the access information for the host device;

failing to find the access information for the host device in the access information database; and

forwarding the access control message to a neighboring device.

46. The method of claim 40, wherein the access information comprises:

a token identifier; and

an authentication key.

47. The method of claim 46, wherein the access control message includes the token identifier.

48. The method of claim 46, wherein the access information further comprises an expiration date for the authentication key.

49. The method of claim 48, wherein determining whether the host device is authorized to access the shared tree comprises:

determining that the authentication key has expired based upon the expiration date for the authentication key; and

determining that the host device is not authorized to access the shared tree.

50. The method of claim 48, wherein determining whether the host device is authorized to access the shared tree comprises:

determining that the authentication key has expired based upon the expiration date for the authentication key; and

forwarding the access control message to a neighboring device.

51. The method of claim 40, wherein determining whether the host device is authorized to access the shared tree comprises:

authenticating the host device using the access information and a predetermined authentication scheme; and

determining whether the host device is authorized to access the shared tree based upon authenticating the host device using the access information and the predetermined authentication scheme.

52. The method of claim 51, wherein authenticating the host device using the access information and the predetermined authentication scheme comprises:

receiving authentication information from the host device; and

authenticating the host device based upon the access information and the authentication information received from the host device.

53. The method of claim 52, wherein the authentication information comprises a digital signature, and wherein authenticating the host device based upon the access information and the authentication information received from the host device comprises:

verifying the digital signature using the access information and a predetermined digital signature scheme.

54. The method of claim 53, wherein the predetermined digital signature scheme comprises a keyed hash function.

55. The method of claim 54, wherein the keyed hash function comprises IPsec AH with HMAC-MD5.

56. The method of claim 54, wherein the keyed hash function comprises IPsec AH with HMAC-SHA1.

57. The method of claim 51, wherein determining whether the host device is authorized to access the shared tree based upon authenticating the host device using the access information and the predetermined authentication scheme comprises:

determining that authentication failed;

determining that the host device is not authorized to access the shared tree.

58. The method of claim 57, further comprising:

forwarding the access control message to a neighboring device.

59. The method of claim 51, wherein determining whether the host device is authorized to access the shared tree based upon authenticating the host device using the access information and the predetermined authentication scheme comprises:

determining that authentication succeeded; and

determining that the host device is authorized to access the shared tree.

60. The method of claim 40, further comprising:

establishing a security association with the host device using the access information upon determining that the host device is authorized to access the shared tree.

61. An apparatus comprising:

authenticating logic operably coupled to authenticate a host device;

access logic operably coupled to generate access information for the host device; and

distribution logic operably coupled to distribute the access information to the host device and to a designated device for the host device.

62. The apparatus of claim 61, wherein the access logic is operably coupled to generate an access token for the host device including the access information.

63. The apparatus of claim 62, wherein the access token comprises:

a group identifier for identifying a multicast group;

a host identifier for identifying the host device;

a token identifier for identifying the access token;

an authentication key for the host device;

an expiration date for the authentication key;

a server identifier for identifying a key server; and

a public key for a key server.

64. The apparatus of claim 61, wherein the distribution logic comprises:

group key management logic operably coupled to send the access information to the host device.

65. The apparatus of claim 61, wherein the distribution logic comprises:

unicasting logic operably coupled to send the access information to the designated device using a unicast mechanism.

66. The apparatus of claim 61, wherein the distribution logic comprises:

multicasting logic operably coupled to send the access information to the designated device using a multicast mechanism.

67. The apparatus of claim 61, wherein the distribution logic comprises:

broadcasting logic operably coupled to send the access information to the designated device using a broadcast mechanism.

68. A computer program for controlling a computer system, the computer program comprising:

authenticating logic programmed to authenticate a host device;

access logic programmed to generate access information for the host device; and

distribution logic programmed to distribute the access information to the host device and to a designated device for the host device.

69. The computer program of claim 68, wherein the access logic is programmed to generate an access token for the host device including the access information.

70. The computer program of claim 69, wherein the access token comprises:

a group identifier for identifying a multicast group;

a host identifier for identifying the host device;

a token identifier for identifying the access token;

an authentication key for the host device;

an expiration date for the authentication key;

a server identifier for identifying a key server; and

a public key for a key server.

71. The computer program of claim 68, wherein the distribution logic comprises:

group key management logic programmed to send the access information to the host device.

72. The computer program of claim 68, wherein the distribution logic comprises:

unicasting logic programmed to send the access information to the designated device using a unicast mechanism.

73. The computer program of claim 68, wherein the distribution logic comprises:

multicasting logic programmed to send the access information to the designated device using a multicast mechanism.

74. The computer program of claim 68, wherein the distribution logic comprises:

broadcasting logic programmed to send the access information to the designated device using a broadcast mechanism.

75. An apparatus comprising:

receiving logic operably coupled to receive access information for joining a multicast group from an access information server; and

access logic operably coupled to generate an access control message for joining the multicast group using the access information and send the access control message to a designated device for joining the multicast group.

76. The apparatus of claim 75, wherein the access information comprises:

a token identifier; and

an authentication key.

77. The apparatus of claim 76, wherein the access logic is operably coupled to include the token identifier in the access control message.

78. The apparatus of claim 75, wherein the access logic is operably coupled to generate authentication information using the access information and send the authentication information to the designated device.

79. The apparatus of claim 78, wherein the access logic is operably coupled to generate the authentication information by generating a digital signature using the access information and a predetermined digital signature scheme.

80. The apparatus of claim 79, wherein the predetermined digital signature scheme comprises a keyed hash function.

81. The apparatus of claim 80, wherein the keyed hash function comprises IPsec AH with HMAC-MD5.

82. The apparatus of claim 80, wherein the keyed hash function comprises IPsec AH with HMAC-SHA1.

83. The apparatus of claim 76, wherein the access information further comprises a token identifier.

84. The apparatus of claim 83, wherein the access logic is operably coupled to include the token identifier in the access control message.

85. The apparatus of claim 84, wherein the access control message is an Internet Group Management Protocol (IGMP) join request message including the token identifier.

86. The apparatus of claim 75, wherein the access logic is operably coupled to establish a security agreement with the designated device using the access information.

87. A computer program for controlling a computer system, the computer program comprising:

receiving logic programmed to receive access information for joining a multicast group from an access information server; and

access logic programmed to generate an access control message for joining the multicast group using the access information and send the access control message to a designated device for joining the multicast group.

88. The computer program of claim 87, wherein the access information comprises:

a token identifier; and

an authentication key.

89. The computer program of claim 88, wherein the access logic is programmed to include the token identifier in the access control message.

90. The computer program of claim 87, wherein the access logic is programmed to generate authentication information using the access information and send the authentication information to the designated device.

91. The computer program of claim 90, wherein the access logic is programmed to generate the authentication information by generating a digital signature using the access information and a predetermined digital signature scheme.

92. The computer program of claim 91, wherein the predetermined digital signature scheme comprises a keyed hash function.

93. The computer program of claim 92, wherein the keyed hash function comprises IPsec AH with HMAC-MD5.

94. The computer program of claim 92, wherein the keyed hash function comprises IPsec AH with HMAC-SHA1.

95. The computer program of claim 88, wherein the access information further comprises a token identifier.

96. The computer program of claim 95, wherein the access logic is programmed to include the token identifier in the access control message.

97. The computer program of claim 96, wherein the access control message is an Internet Group Management Protocol (IGMP) join request message including the token identifier.

98. The computer program of claim 87, wherein the access logic is programmed to establish a security agreement with the designated device using the access information.

99. An apparatus comprising:

receiving logic operably coupled to receive an access control message from a host device;

access logic operably coupled to determine whether the host device is authorized to access a shared multicast distribution tree based upon access information for the host device; and

joining logic operably coupled to join the shared tree on behalf of the host device if the access logic determines that the host device is authorized to access the shared tree.

100. The apparatus of claim 99, wherein the access logic is operably coupled to obtain the access information for the host device from an access information server.

101. The apparatus of claim 100, wherein the access logic is operably coupled to obtain the access information for the host device from the access information server prior to receiving the access control message from the host device.

102. The apparatus of claim 100, wherein the access logic is operably coupled to obtain the access information for the host device from the access information server after receiving the access control message from the host device.

103. The apparatus of claim 99, further comprising an access information database.

104. The apparatus of claim 103, wherein the access logic is operably coupled to search the access information database for the access information for the host device and determine that the host device is not authorized to access the shared tree upon failing to find the access information for the host device in the access information database.

105. The apparatus of claim 103, wherein the access logic is operably coupled to search the access information database for the access information for the host device and forward

the access control message to a neighboring device upon failing to find the access information for the host device in the access information database.

106. The apparatus of claim 99, wherein the access information comprises:
a token identifier; and
an authentication key.

107. The apparatus of claim 106, wherein the access control message includes the token identifier.

108. The apparatus of claim 106, wherein the access information further comprises an expiration date for the authentication key.

109. The apparatus of claim 108, wherein the access logic is operably coupled to determine whether the host device is authorized to access the shared tree based upon the expiration date for the authentication key.

110. The apparatus of claim 109, wherein the access logic is operably coupled to determine that the host device is not authorized to access the shared tree upon determining that the authentication key has expired based upon the expiration date for the authentication key.

111. The apparatus of claim 109, wherein the access logic is operably coupled to forward the access control message to a neighboring device upon determining that the authentication key has expired based upon the expiration date for the authentication key.

112. The apparatus of claim 99, wherein the access logic is operably coupled to authenticate the host device using the access information and a predetermined authentication scheme.

113. The apparatus of claim 112, wherein the access logic is operably coupled to receive authentication information from the host device and authenticate the host device based upon the access information and the authentication information received from the host device.

114. The apparatus of claim 113, wherein the authentication information comprises a digital signature, and wherein the access logic is operably coupled to verify the digital signature using the access information and a predetermined digital signature scheme.

115. The apparatus of claim 114, wherein the predetermined digital signature scheme comprises a keyed hash function.

116. The apparatus of claim 115, wherein the keyed hash function comprises IPsec AH with HMAC-MD5.

117. The apparatus of claim 115, wherein the keyed hash function comprises IPsec AH with HMAC-SHA1.

118. The apparatus of claim 112, wherein the access logic is operably coupled to determine that the host device is not authorized to access the shared tree upon determining that the authentication failed.

119. The apparatus of claim 118, wherein the access logic is operably coupled to forward the access control message to a neighboring device upon determining that the authentication failed.

120. The apparatus of claim 112, wherein the access logic is operably coupled to determine that the host device is authorized to access the shared tree upon determining that the authentication succeeded.

121. The apparatus of claim 99, wherein the access information is operably coupled to establish a security association with the host device using the access information upon determining that the host device is authorized to access the shared tree.

122. A computer program for controlling a computer system, the computer program comprising:

receiving logic programmed to receive an access control message from a host device;

access logic programmed to determine whether the host device is authorized to access a shared multicast distribution tree based upon access information for the host device; and

joining logic programmed to join the shared tree on behalf of the host device if the access logic determines that the host device is authorized to access the shared tree.

123. The computer program of claim 122, wherein the access logic is programmed to obtain the access information for the host device from an access information server.

124. The computer program of claim 123, wherein the access logic is programmed to obtain the access information for the host device from the access information server prior to receiving the access control message from the host device.

125. The computer program of claim 123, wherein the access logic is programmed to obtain the access information for the host device from the access information server after receiving the access control message from the host device.

126. The computer program of claim 122, further comprising an access information database.

127. The computer program of claim 126, wherein the access logic is programmed to search the access information database for the access information for the host device and determine that the host device is not authorized to access the shared tree upon failing to find the access information for the host device in the access information database.

128. The computer program of claim 126, wherein the access logic is programmed to search the access information database for the access information for the host device and forward the access control message to a neighboring device upon failing to find the access information for the host device in the access information database.

129. The computer program of claim 122, wherein the access information comprises:
a token identifier; and
an authentication key.

130. The computer program of claim 129, wherein the access control message includes the token identifier.

131. The computer program of claim 129, wherein the access information further comprises an expiration date for the authentication key.

132. The computer program of claim 131, wherein the access logic is programmed to determine whether the host device is authorized to access the shared tree based upon the expiration date for the authentication key.

133. The computer program of claim 132, wherein the access logic is programmed to determine that the host device is not authorized to access the shared tree upon determining that the authentication key has expired based upon the expiration date for the authentication key.

134. The computer program of claim 132, wherein the access logic is programmed to forward the access control message to a neighboring device upon determining that the authentication key has expired based upon the expiration date for the authentication key.

135. The computer program of claim 122, wherein the access logic is programmed to authenticate the host device using the access information and a predetermined authentication scheme.

136. The computer program of claim 135, wherein the access logic is programmed to receive authentication information from the host device and authenticate the host device based upon the access information and the authentication information received from the host device.

137. The computer program of claim 136, wherein the authentication information comprises a digital signature, and wherein the access logic is programmed to verify the digital signature using the access information and a predetermined digital signature scheme.

138. The computer program of claim 137, wherein the predetermined digital signature scheme comprises a keyed hash function.

139. The computer program of claim 138, wherein the keyed hash function comprises IPsec AH with HMAC-MD5.

140. The computer program of claim 138, wherein the keyed hash function comprises IPsec AH with HMAC-SHA1.

141. The computer program of claim 135, wherein the access logic is programmed to determine that the host device is not authorized to access the shared tree upon determining that the authentication failed.

142. The computer program of claim 141, wherein the access logic is programmed to forward the access control message to a neighboring device upon determining that the authentication failed.

143. The computer program of claim 135, wherein the access logic is programmed to determine that the host device is authorized to access the shared tree upon determining that the authentication succeeded.

144. The computer program of claim 122, wherein the access information is programmed to establish a security association with the host device using the access information upon determining that the host device is authorized to access the shared tree.

145. A communication message embodied in a data signal, the communication message comprising a group key for a multicast group and access information for a host device.

146. The communication message of claim 145, wherein the access information comprises:

a token identifier; and

an authentication key.

147. The communication message of claim 146, wherein the access information further comprises an expiration date for the authentication key.

148. The communication message of claim 145, wherein the access information comprises an access token.

149. The communication message of claim 148, wherein the access token comprises:

a group identifier for identifying a multicast group;

a host identifier for identifying the host device;

a token identifier for identifying the access token;

an authentication key for the host device;

an expiration date for the authentication key;

a server identifier for identifying a key server; and

a public key for the key server.

150. A communication message embodied in a data signal, the communication message comprising an access control message including access information for a host device.

151. The communication message of claim 150, wherein the access information comprises a token identifier.

152. The communication message of claim 150, wherein the access information comprises authentication information generated using the access information.